

Information compression for remote readable ID tags

Sergi Horrillo, Elisabet Pérez-Cabré and María S. Millán

Dept. Òptica i Optometria, Universitat Politècnica de Catalunya, Violinista

Vellsolà 37, 08222 Terrassa (Spain)

E-mail: elisabet.perez@upc.edu

Abstract. Optical ID tags have been introduced and described to achieve remote target recognition and identification. Optical ID tags usually contain encrypted signatures to be read out, decrypted and verified. In this paper, new features are introduced so that ID tags can be reliably used for remote detection and verification even if the captured tag is extremely degraded by perspective or optical distortion. Optimization of the ID tag size as well as the number of bits required to display the complex-amplitude information are analyzed and discussed. The highest compression of grey levels, which corresponds to binary ID tags, is studied. Decryption and verification results are provided to analyze the possibilities of the new designed optical ID tags.

1. Introduction

Optical identity (ID) tags have been shown as a useful tool to accomplish the generally difficult task of recognition and identification of moving objects [1-6]. Using optical elements such as light emitters, passive ID tags and receivers, object tracking and also identity verification can be performed remotely and in real-time. The ID tag is commonly an optical code installed on a visible part of the object under surveillance. The optical code consists of either a direct image representative of the object (signature) or an encrypted function that scrambles the image and makes the signature unintelligible. A number of encryption strategies have been applied to a single signature [2,4,7] or a set of identifying factors [3,5-6]. The information distribution over

the ID tag is multiplexed and designed to be redundant in such a way that it can be retrieved from the tag in its original orientation or even rotated or scaled [2-7]. Visible light or other spectral ranges have been considered to illuminate the ID tag and readout its content. The near infrared region (NIR) of the spectrum has been used to increase security over the identification process by hiding the information of the ID tag to direct visual inspection or common acquisition devices in the visible range [3].

Up to now, some features of the original ID tags permit to apply them in controlled situations such as the entrance of vehicles in restricted areas or tracking of parcels on conveyor belts [2-3]. In these situations, environmental constraints can be controlled in some extent and deformations suffered by the ID tag can be mainly reduced to scale variations and/or in-plane rotations. In a more general scenario, tracking of moving objects from any viewpoint implies detection of distorted ID tags due to perspective, or to optical aberrations of the imaging system (e.g. barrel or pincushion distortion). A recent research work in the field of digital object recognition [8], tries to extend the system tolerance to simple geometric transformations of the object to more general polynomial transformations of the spatial coordinates by defining what the authors called implicit moment invariants.

In this paper, we present a novel design of the optical ID tag that substantially improves the identification system robustness against changes of perspective and optical distortions. A template of reference dots on the ID tag permit to extend the distortion tolerance of the proposed tag to the deformations that may occur in case of remote capture. Moreover, the choice of the template permits to simplify the complexity of the optical code so that its size can be significantly reduced in comparison with prior designs. As an additional and not less important novelty, the range of grey levels used to codify the encrypted signature on the ID tag, initially considered as to be 256 in Refs. [2-7], can be limited to a smaller number of quantization levels, so that this study will actually approach the manufacturing process for a real ID tag, and would easily overcome the likely difficult situation of ID tag readout in the presence of noise.

The paper is organized as follows: Section 2 briefly reviews the encryption techniques used in this paper to obtain an encrypted signature. It also introduces the procedure to synthesise an ID tag from the encrypted function. Section 3 focuses on retrieving the information included in the ID tag by means of a reading mask. The algorithms that make the ID tag resistant against deformations caused by perspective and optical distortions are presented in section 4, along with some of the most relevant verification results. Section 5 introduces the possibility of reduce the range of grey levels used to codify the ID tag information, evaluates its effects on the decryption process and provides verification results for deformed ID tags that display the complex-amplitude information with just 1 or 2-bits. Finally, the main points of this research work are summarized in the Conclusions.

2. ID tag synthesis

Two consecutive steps are involved to synthesise an ID tag. First of all, an encryption technique is firstly applied to the primary image used as a signature. This ciphering step can be accomplished by using a number of methods [6,9-11] and gives a noise-like appearance to the encrypted signature that prevents its recognition from direct visual inspection. The encrypted information is distributed over the ID tag area in a second step. Former designs of the ID tag [2-7] allowed us to read out the ciphered information and to decrypt it even if the captured tag was scaled or rotated. A novel ID tag design is presented in this paper. It will permit to retrieve the information not only from scaled and rotated versions but also from extremely deformed captured ID tags. In this section, both steps, the encryption and the novel ID tag distribution, are described in detail.

2.1 Encryption

Optical encryption systems have been reviewed in the literature [5,6]. For a single input, a number of encryption techniques are based on the double random phase encryption (DRPE), a method introduced in the pioneering work of Refregier and Javidi [8]. Recently, the linearity of this proposal has been proved to be the reason of some vulnerable aspects to intruder attacks

[12,6]. This vulnerability appears when it is assumed an ideal mathematical version of the DRPE technique and all the process is carried out in digital form. However, in a real optical implementation, the physical complexity of the system contributes with additional challenges to the opponent. Some variants of the DRPE technique have been recommended to increase the security and robustness of the encryption system. Among them, Towghi et al. [10] modified the linear encoding technique of the DRPE by introducing a nonlinear encoding. This proposal, named the fully-phase encryption (FPE), is used in this work. Let us recall it briefly.

Let the real valued function $f(x,y)$ be the signature to be encrypted that is normalised ($0 \leq f(x,y) \leq 1$) and sampled to have a total amount of pixels N (Fig. 1a). Let (x,y) and (u,v) be the coordinates in the spatial and in the frequency domains, respectively. A phase-encoded version of the primary image, $\exp[i\pi f(x,y)]$, is used as the input of the encryption process. The phase-encoded image is firstly multiplied by the phase mask $\exp[i2\pi p(x,y)]$, where $p(x,y)$ is a white sequence randomly distributed in $[0,1]$. This product is then convolved by a function $h(x,y)$, which is the impulse response of a phase-only transfer function $H(u,v) = \exp[i2\pi b(u,v)]$. Function $b(u,v)$ is a uniform random distribution over the range $[0,1]$. Thus, the fully-phase encrypted signature, $\psi(x,y)$, is a complex-valued function given by

$$\psi(x,y) = \left\{ \exp[i\pi f(x,y)] \exp[i2\pi p(x,y)] \right\} * h(x,y), \quad (1)$$

where symbol $(*)$ represents convolution.

The encryption procedure converts the primary image into a stationary white noise that does not reveal the appearance of the input signature (Fig. 1b).

The performance of the FPE method [10] will be compared to the DRPE technique [9] when both encryption procedures are applied at some point of this paper. The latter differs from the first in the function used as the input of the encryption method. While the FPE uses a phase

encoded version of the signature $\exp[i\pi f(x,y)]$, the DRPE uses just the primary image $f(x,y)$ [9].

2.2 Information distribution on the ID tag

The synthesis of the ID tag is achieved by both multiplexing the information of the encrypted function $\psi(x,y)$ and taking advantage of the ID tag topology [2-7]. Let us consider the complex-valued encrypted function $\psi(x,y)$ (Eq. 1) in array notation $\psi(t) = |\psi(t)| \exp[i\phi_\psi(t)]$ where $t = 1, 2, \dots, N$. We build two real valued vectors that are to be encoded greyscale: the magnitude vector $|\psi(t)|$ and the phase vector $\phi_\psi(t)$ (Fig. 1b). It is preferable to print the phase content of $\psi(x,y)$ in greyscale variations rather than in phase to avoid sabotage by, for instance, sticking an adhesive transparent tape on the tag. The information included in the ID tag is distributed in two optical disks. One disk corresponds to the magnitude $|\psi(t)|$, and the other contains the phase vector $\phi_\psi(t)$. In both disks the information is distributed in a similar way, so that the information of a given pixel (t) corresponds to an angular sector in the optical code (Fig. 1c). Thus, the readout of the ciphered information will be tolerant to variations in scale up to a certain range. For encrypted functions with a large number of pixels, as the example of Fig. 1 (30x30 pixels size), information needs to be distributed by using different concentric rings to ensure enough readable pixels in each sector (Fig. 1c). Consequently, the tolerance to scale variations will be reduced in accordance to the number of concentric rings used in the ID tag. As we go far away from the centre, the radius of the concentric rings increases always by the same amount, ΔR , while the width of the angular sectors, ω_i , decreases from a given ring to the next one in order to keep the number of pixels constant (Fig. 1c). Values of parameters ΔR and ω_i have to be fixed according to a particular application and its tolerance requirements. As shown in the example of Fig. 1c, the central circular area of radius R of both, the amplitude and phase disks, is not further divided into angular sectors.

Using the procedure described, the information is redundantly written, so that a natural resistance to noise and other damages due to common handling (e.g. scratches) would be likely obtained.

Regarding tolerance to scale variations, the topology of both disks is designed in this paper differently to previous proposals. In the past, only a half of the circles was used for such a purpose [2-7]. The other semicircles were used to obtain rotation-invariance by writing both vectors, $|\psi(t)|$ and $\varphi_\psi(t)$, in the radial direction and repeating them angularly [2-7]. The rotation-invariant region of the ID tag was responsible for having a bigger size than the original size of the signature. Thus, for instance, in the case of the signature of Fig. 1a (30x30 pixel size) an enormous tag of 1830x3660 pixels was generated. To optimize the dimensions of the ID tag, our proposal in this paper does not include these rotation-invariant semicircles. We introduce a set of reference white circular dots instead. As it will be justified in section 3.1, the minimum number of reference dots is determined by the kind of transformation used to compensate for the deformation of the captured ID tag.

Figure 2a depicts the location of the 15 reference white dots (template) that are very useful in the remote detection and capturing of an ID tag. These dots are distributed in the free areas of the rectangular ID tag. Four dots are located at the corners of the ID tag (labelled 1, 2, 14 and 15). Nine dots, grouped in three sets of three, are at the centre of the disks (groups labelled a and c) and in the upper central part of the ID tag (group b). Finally, two more reference dots are located at the bottom central part of the tag (group d). It is necessary to introduce an asymmetry in the template (different number of dots in groups b and d) in order to establish a bijective function between the reference template of the original ID tag and the remotely captured ID tag. All the 15 reference dots of the template have a uniform value which is set to the maximum grey level (white) to make their detection easy.

The final ID tag synthesised from the encrypted signature of Fig. 1b is depicted in Fig. 2b. For this case of a 30x30 pixels signature, the synthesised ID tag has 470x930 pixels, which corresponds to a 7% of the total area of the original ID tag. The generated ID tag is located on

an accessible part of the object under surveillance, so that a receiver can capture it from a remote distance. If necessary, the ID tag could be generated by using proper materials that make the ID tag only visible under NIR illumination [3]. In such a case, a detector sensible to the NIR spectrum needs to be used to read the information of the ID tag.

3. Information readout and verification

Once the receiver captures the ID tag, the object authentication implies the readout of the information included in the ID tag, its decryption and its verification. In the capturing process, degradation due to rotations, scale variations, shearing, perspective, distortion of the optical imaging system and so on can severely modify the geometry of the ID tag. To satisfactorily retrieve the information, it is important to ensure that the magnitude and phase values of the encrypted function $\psi(x,y)$ are correctly readout without additional alterations. Thus, it is advisable to avoid digital transformation of the captured ID tag to compensate for deformations because digital interpolations would be involved in the process.

In this section, we firstly detail how a transformation matrix \mathbf{T} , which accounts for the deformations of the captured ID tag, can be determined. Afterwards, we describe the procedure to retrieve the information from the tag without additional interpolations, and finally the decryption and verification processes are explained.

It is assumed that the receiver has a complete knowledge of the tag topology and the geometry with which the information is distributed in it.

3.1 Determination of the transformation matrix \mathbf{T}

To calculate the transformation matrix \mathbf{T} to compensate for possible degradations of the captured ID tag, we use the information concerning the fifteen reference dots distributed over the rectangular optical tag (Fig. 2). All the dots of the template are set to the maximum grey level (white). We apply a threshold level of 85% of the maximum grey level of the captured ID tag that permit to roughly detect the template. A digital image processing is carried out to distinguish between the sought reference dots and the unwanted elements that still remain in the

binary image. The binary objects are digitally filled to obtain solid areas and an erosion operation with a circular structural element is applied to remove thin objects. Only the objects that remain in the eroded image are considered and they are reconstructed as they were before erosion. An additional threshold level regarding the object size is applied to eliminate small objects. Due to deformations in the capturing process, both reference dots and circular sectors appear with modified shapes. Usually, dots are transformed into ellipses. Thus, the final criterion to select the binary objects that belongs to the template is the comparison of the area of the object (number of pixels in the image) with the area of a hypothetical ellipse that has the same length of the major and minor axes of the object.

Once the template is detected, it is necessary to identify the reference dots in order to determine their correspondence with each dot of the original ID tag. The non-uniform distribution of the dots (see Fig. 2) permits to achieve this purpose. Groups a, b and c (Fig. 2a) are identified by looking for the closest distances between dots. From them, point P is determined as the barycentre of the triangle formed by these groups of dots. Considering the other detected dots, group d is identified and the middle point between its two dots is computed. This point is labelled as Q in Fig. 2a. The relative position of point P and Q permits to number all the dots according to their location and establishes their relationship with the dots of an ideal non-rotated ID tag.

The identification of the fifteen reference dots on the captured ID tag is a necessary step to determine the degradation suffered by the tag, and, therefore, to calculate the transformation matrix \mathbf{T} that links the original and the captured ID tag. According to Ref. [13], the transformation introduced by a camera can be modelled by a polynomial function. In order to cover a wide range of deformations due to perspective and distortion of the optical imaging system, and from our preliminary studies, third order polynomials achieve a good approximation between the original and the deformed patterns in the vast majority of cases. Thus, we choose this approximation to obtain a bijective transformation.

For a third order polynomial approximation, the transformation is defined by a matrix \mathbf{T} that satisfies

$$\begin{bmatrix} \alpha_j & \beta_j \end{bmatrix} = \begin{bmatrix} 1 & x_j & y_j & x_j y_j & x_j^2 & y_j^2 & y_j x_j^2 & x_j y_j^2 & x_j^3 & y_j^3 \end{bmatrix} \mathbf{T} \quad (2)$$

where (x_j, y_j) and (α_j, β_j) with $j = \{0, 1, 2, \dots, q\}$ are the coordinates in the initial and the

final spaces, respectively. Matrix \mathbf{T} has 10 pairs of coefficients, $\mathbf{T} = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_9 \\ b_0 & b_1 & b_2 & \dots & b_9 \end{bmatrix}^t$

and superindex t indicates the transpose of the matrix. Theoretically, a minimum of ten reference points ($q=9$) are necessary to solve Eq. (2) and know the coefficients of the transformation matrix \mathbf{T} . As aforementioned, we have added a template of fifteen reference dots on the ID tag to assure that the minimum number of reference points would be covered even if the deformation of the tag was severe or if some dots were cut.

The central coordinates of the dots of the template (usually, fifteen of them) detected and identified as described above, will be used to determine the transformation matrix \mathbf{T} . Once this matrix is known, the bijective function described in Eq. (2) can be applied to transform a given image from one space to another [14].

3.2 Reading mask and information readout

Once the deformation of the captured ID tag has been determined, the following step is to read the information contained in the tag according to its acquired geometry. To avoid additional alteration of the information of the tag, we do not transform the captured ID tag back to its original geometry because this process will imply interpolation of the pixel values. We propose instead to synthesise a reading mask that will adapt its shape to the distorted ID tag. Figure 3a shows an example of this reading mask. It shows a structure similar to the ID tag of (Fig. 2b). It contains two disks divided into concentric rings and each concentric ring is subdivided in turn into small circular sectors.

The bijective transformation of Eq. (2) is applied to the reading mask so that it adapts its geometry to the captured ID tag (Fig. 3c and 3d). Therefore, direct readout of the magnitude and phase values can be achieved. The fact that the circular sectors of the reading mask are smaller than the ones on the ID tag is intended to increase the reliability of the reading process

especially when strong deformations occur. In such a case, some overlapping between the values of lateral sectors may take place giving rise to errors in the reading process. The area for the reading circular sectors is approximately 40% of the corresponding circular sectors of the ID tag. It accounts for the number of pixels (around 70 pixels) we want to take into account for a reliable retrieval of values of the magnitude and phase of the pixels. The final value for each pixel of the magnitude vector $|\psi(t)|$ and the phase vector $\phi_\psi(t)$ is obtained by computing the median value of the set of read pixels.

3.3 Signature decryption and verification

Retrieved vectors $|\psi(t)|$ and $\phi_\psi(t)$ are rearranged in matrix notation to obtain the encrypted function $\psi(x, y)$. Then, the FPE method is applied to function $\psi(x, y)$ to decrypt the signature hidden on the ID tag. The complex conjugate of both random phase masks, $\exp[-i2\pi p(x, y)]$ and $\exp[-i2\pi b(u, v)]$ are needed for decryption, and usually they are referred to as keys. The Fourier transformed encrypted function $FT\{\psi(x, y)\}$ is multiplied by the complex conjugate phase key, $\exp[-i2\pi b(u, v)]$. Then, the result is inverse Fourier transformed to produce the output $\exp[i\pi f(x, y)]\exp[i2\pi p(x, y)]$, and this result is multiplied by the second complex conjugated phase key, $\exp[-i2\pi p(x, y)]$. The primary image $f(x, y)$ can be visualized as an intensity distribution by extracting the phase of $\exp[i\pi f(x, y)]$ and dividing by the normalization constant π [9].

As opposed to the DRPE [8], two keys are needed to retrieve the signature when the FPE technique is applied. In that sense, the system security is increased. For the DRPE [8], only the first phase mask, $\exp[-i2\pi b(u, v)]$ is necessary for decryption. The output $f(x, y)\exp[i2\pi p(x, y)]$ is produced in this decryption method and provided $f(x, y)$ was a

real positive function, an intensity sensitive device, such a CCD camera, would register the hidden signature.

Authentication of the obtained signature will be positive if a comparison with a previously stored reference signature satisfies a given degree of similarity. The measurement of similarity between two images can be achieved by different procedures, among them, correlation [15] or the root-mean-square error (*RMS*) [14]. The latter has been chosen in this work to evaluate the system performance. The *RMS* is defined for an $M \times N$ image as

$$RMS = \left\{ \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x, y) - f_{ref}(x, y)]^2 \right\}^{\frac{1}{2}}, \quad (3)$$

where $f_{ref}(x, y)$ is the reference signature and $f(x, y)$ is the decrypted signature from the captured ID tag.

4. Signature retrieval from severely deformed ID tags

In this section, we show simulation results that prove the reliability of the proposed ID tag. We test the new ID tag design under a variety of situations corresponding to the expected deformations that could be introduced in the capturing process by a remote receiver. To summarize the experiences we have analyzed, we only show some of the most interesting results, to show the limits of the system and at the same time, to present results when the ID tag has suffered strong degradation, even stronger than what one can expect from a common capturing system.

4.1 ID tag modified by perspective

In a general situation, the relative position of the receiver and the object under surveillance determines the perspective of the captured ID tag. Figure 3b depicts the angles considered to model the deformation introduced by perspective for a flat object, such as the ID tag [13]. Figure 4 shows two examples of the captured ID tag viewed from different points or perspectives. Apart from deformations, we also consider the optical inversion done by the

imaging system of the receiver. Figure 4a shows an ID tag corresponding to angles $\theta = 70^\circ$ and $\varphi = -30^\circ$, and figure 4b corresponds to $\theta = 40^\circ$ and $\varphi = -15^\circ$. Following the readout and decryption processes formerly described, the decrypted signature is obtained and the value RMS is computed in each case. Both examples achieve small values of the RMS , which imply fairly good decryptions of the signature as it is shown in the upper left corner of each ID tag. However, the decrypted image obtained when the ID tag is reoriented back to its original position by interpolation is unacceptable as it is shown in the bottom left corner of figure 4a. The obtained noisy signal impedes the recognition of the signature and confirms the better performance of the reading mask in comparison with the interpolation of the captured ID tag.

4.2 Distorted ID tag by the optical imaging system

The optical imaging system of a camera may introduce distortion for wide field of view if it is not well-corrected. We simulate this optical aberration in order to consider a more realistic approach to the remote capturing of the ID tag. In case of distortion, both barrel and pincushion aberrations can be modelled by [16]

$$\begin{cases} x = x + a \cdot \rho^3 & \text{if } x \geq 0 \\ x = x - a \cdot \rho^3 & \text{if } x < 0 \end{cases} \quad \begin{cases} y = y + a \cdot \rho^3 & \text{if } y \geq 0 \\ y = y - a \cdot \rho^3 & \text{if } y < 0 \end{cases}, \quad (4)$$

where $a < 0$ corresponds to barrel distortion and $a > 0$ to pincushion, and ρ defines distance in polar coordinates (see figure 3b).

By using equation (4), we have simulated an ID tag affected by both types of distortion. Figure 5 shows two examples of this situation. In both cases, the captured ID tag suffers from severe distortion, stronger than what one could expect from a common optical camera system. The ID tag shown in figure 5a is affected by barrel distortion, while the ID tag in figure 5b is distorted by pincushion. After the readout and decryption processes, both examples obtain fairly good results in terms of the RMS parameter and the retrieved signature, as it can be noticed from the signatures placed on the upper left corner of the ID tags. For the case corresponding to barrel distortion, interpolation of the captured ID tag to its original position is computed for comparison. The resulting decrypted image is shown in the bottom left corner of the ID tag.

Again, this result clearly points out the advantages of using a reading mask to readout the information included in the tag, instead of digital interpolations of the captured ID tag.

5. ID tags reproduced with a limited number of grey levels

For practical purposes, a reduction in the number of grey levels used to codify the encrypted information on the ID tag would permit a more versatile optical tag in two senses. On the one hand, the devices used to reproduce the ID tags would produce more reliable optical tags since the number of grey levels that are actually reproduced in practice is usually lower than the number stated by the manufacturer and would not probably reach 256 grey levels as it has been assumed so far. On the other hand, the ID tag remote readout would be done in more relaxed conditions provided the number of grey levels was reduced. Ideally, a binary ID tag would be easily detected in a general situation and particularly under the presence of noise. Taking into account this consideration, we have carried out a study to evaluate the number of grey levels needed to reproduce the magnitude and phase codes of the ID tag without affecting the identification system performance. The range of grey levels, which depends on the number of bits used to codify the information, will have a direct repercussion on the applied encryption method. To evaluate this effect, the performance of two encryption methods, the DRPE [8] and the FPE [9], has been compared. The analysis of the decryption results has been carried out when the number of bits used to reproduce the magnitude and the phase of the encrypted information is reduced from 8-bit to 1-bit (binary) functions. The retrieved signature and the original primary image have been compared in terms of the *RMS* (Eq. 3) for both encryption algorithms.

Let us consider the following situation: a binary amplitude distribution (left optical disk in the example of figure 6a) and a number of grey levels for the phase information (right optical disk with 8 different grey levels in figure 6a). In the ID tag reading process, the receiver assigns the grey level values of the phase code to the same number of discrete phase values ranging from $[-\pi, \pi]$. In the same way, the system assigns the binary values of the amplitude code to two quantized amplitude values. Let us firstly consider that these two quantized amplitude values

are $\{0,1\}$. If the system performs so, the complex-amplitude encrypted function will have drastically discarded the amount of available information provided by the phase code, since half of the pixels of the amplitude information have a null value on average. As a result, the decrypted signal when the FPE is applied is noisy and hardly depicts the sought signature (see figure 6b).

However, if the binary values of the amplitude code of the ID tag are assigned to two different quantized non-zero values, for instance $\{1,2\}$, the retrieved image will much resemble the original signature (see Fig. 6c) and a positive verification would be achieved.

This example points out the need of determining the best amplitude value assignation for the grey levels used to represent the amplitude information on the ID tag, in a similar way as an assignation of phase values is carried out for the grey levels used to represent the phase code. Figure 7a graphs the *RMS* curves versus an assigned minimum value k for a binary representation $\{k, 255\}$ of the amplitude code, considering different numbers of grey levels for the phase representation. The FPE technique is applied for encryption and decryption. Parameter k varies between zero and the maximum grey level chosen for the binary case. In our assignment the maximum grey level is established to 255, and thus, parameter k ranges from 0 up to 255. Figure 7a shows that the *RMS* value is significantly low if value k is chosen around a mid value of the discretization gap. That is, around 128 in the given example.

Figure 7b shows a similar graph for a 2-bit representation of the amplitude. Amplitude values assigned to the 4 different grey levels are $\{k, \frac{1}{3}255, \frac{2}{3}255, 255\}$, where k ranges from 0 up to $\frac{1}{3}255$. From the *RMS* curves depicted in figure 7b, one can observe that again, the minimum *RMS* values are obtained for k values around the middle point of the grey level gap, i.e. $\frac{1}{2}(\frac{1}{3}255)$, even though the variations of the curve are very subtle.

Finally, figure 7c shows the results corresponding to a 3-bit representation of the amplitude code. The most remarkable result provided by this graph is that *RMS* variations are not noticeable for this number of grey levels. A similar conclusion can be stated for similar representations corresponding to larger amounts of bits. This result is in accordance with the

fact that the number of pixels with a null value for a 3-bit amplitude representation has been reduced to $\frac{1}{8}$ on average, and they have a small influence on the final decryption result. In figures 7a to 7c it can be seen that a binary phase code produces bad results in general. Four or eight grey levels for the phase code are much better.

Figure 8 plots the results obtained for the *RMS* value versus the number of grey levels utilized to codify the amplitude distribution of the encrypted function on the ID tag. Several curves are obtained corresponding to the different number of grey levels used to reproduce the phase distribution on the ID tag. Figure 8a shows the results when the DRPE method is applied while figure 8b corresponds to the FPE technique. Both graphs depict a similar behaviour. From about eight phase quantization levels on, the *RMS* remains approximately constant with the number of amplitude grey levels. A reduction in the number of phase quantization levels generally corresponds to an important increase of the *RMS*, implying a rather noisy or unacceptable deciphering of the hidden signature. Comparing both encryption algorithms, the FPE method performs better than the DRPE in all the considered cases, so that we can state that the FPE technique is best suitable than the DRPE when trying to reduce the number of bits to codify the information on the ID tag.

Several decrypted signatures are presented in figure 8 for a number of representative cases. In general, one can appreciate that it is important to preserve the phase information of the encrypted signature since the decryption of the primary image is retrieved with a smaller *RMS* value. For a given number of bits to reproduce the phase, the *RMS* value does not change significantly with the number of bits used to reproduce the amplitude, except for the case of 1 or 2 bits.

Finally, figure 9 provides some examples of severely deformed ID tags, which have a limited number of grey levels to reproduce both, the magnitude and the phase distribution of $\psi(x, y)$.

In the upper corner of the ID tags the satisfactorily retrieved signature is also shown.

Figure 9a and 9b depict ID tags deformed by barrel and pincushion distortion, respectively. In both situations, the amplitude and phase information are both reproduced with 3-bits (or 8 grey

levels). Figure 9c shows an example of ID tag modified by perspective for which only 2-bits (4 grey levels) are considered to reproduce both the amplitude and the phase distributions. Finally, Figure 9d presents an ID tag deformed simultaneously by perspective and distortion. In this example, the phase information is reproduced with 2-bits (4 grey levels) while the amplitude is binary. In all the cases shown in figure 9, the retrieved signatures are clearly recognisable although the level of noise increases inversely proportional to the number of bits used to convey the information. We have shown that even for ID tags deformed by perspective and distortion simultaneously, it is possible to significantly reduce the number of grey levels used to reproduce the complex information of the encrypted signature without affecting the final verification result.

Conclusions

A novel proposal of experimentally feasible ID tags has been presented in this work. The new features introduced in the ID tag design increase its distortion-tolerance over a number of possible deformations that usually occur in remote detection. Not only are scale variations and in-plane rotations compensated for in the information reading and verification processes, but also extreme modifications due to perspective or distortion of the optical imaging receiver.

A significant reduction of the ID tag area is achieved along with an important reduction of the number of bits used to display the grey levels of the complex-amplitude encrypted information on the ID tag. Both characteristics will permit to manufacture more reliable ID tags and reduce its production cost.

Concerning the ID tag area, the use of a template of 15 reference dots has permitted to drastically reduce the size of the optical disks of the ID tag. For the example considered in this work (signature shown in figure 1a) the area occupied by the new proposed ID tag (Fig. 2b) corresponds to approximately a 7% of the area occupied by previous designs of the tag reported in Refs [2-7].

Regarding the range of grey levels, simulation results confirm that it is preferable to preserve the phase information of the encrypted signature included in the ID tag, than the amplitude

distribution. For this reason, reduction in the number of grey levels (or bits) used to reproduce the phase information is more critical than the reduction of the number of grey levels used for the amplitude. In the latter case, it is possible to consider binary codes to implement the amplitude information on the ID tag, and still obtain positive verification results.

For two different encryption methods, the fully-phase encryption (FPE) technique shows better decryption and verification results than the double random phase encryption (DRPE) when limiting the number of bits to display the grey levels corresponding to the amplitude and phase distributions on the ID tag. In addition to this, the nonlinear input used for encryption in the FPE technique entails an increased robustness in front of certain intruder attacks in comparison to the DRPE. These results make the FPE technique more attractive to be combined with our proposal.

Analysis and results provided in this paper show the satisfactory performance of the proposed ID tags. The new morphology of the tag permits verification of the information even for extremely degraded captured ID tags due to perspective or optical distortion even when the amplitude and the phase disks are both reproduced with only 2 bits, or when a binary (1-bit) amplitude is considered.

Acknowledgements

This research work has received financial funding from the Spanish Ministerio de Ciencia e Innovación y Fondo FEDER (project DPI2009-08879).

References

- [1] Javidi, B. (2003) "Real-time remote identification and verification of objects using optical ID tags," *Opt. Eng.*, 42, 2346-48.
- [2] Pérez-Cabré, E., Javidi, B. (2005) "Scale and rotation-invariant optical ID tags for automatic vehicle identification and authentication," *IEEE Trans. Veh. Technol.*, 54, 1295-303.
- [3] Pérez-Cabré, E., Millán, M. S., Javidi, B. (2007), "Near infrared multifactor identification tags," *Opt. Exp.*, 15, 15615-27.

- [4] Pérez-Cabré, E., Millán, M. S., Javidi, B. (2007) “Design of distortion-invariant optical ID tags for remote identification and verification of objects,” in *Physics of the Automatic Target Recognition*, Sadjadi, F., Javidi, B. eds., Springer-Verlag, Chap. 12.
- [5] Matoba, O., Nomura, T., Pérez-Cabré, E., Millán, M. S., Javidi, B. (2009) “Optical techniques for information security”, *Proc of the IEEE J.*, 97, 1128-48.
- [6] Millán, M. S., Pérez-Cabré, E. (2010) “Optical Data Encryption,” in *Optical and Digital Image Processing*, Cristobal, G. Shelkens, P. Thienpont, H. Eds., Wiley, Germany (in press).
- [7] Pérez-Cabré, E., Millán, M. S., Javidi, B. (2005) “Remote optical ID tag recognition and verification using fully spatial phase multiplexing,” *Proc. SPIE*, 5986, 508602-1/13.
- [8] Flusser, J., Kautsky, J., Sroubek, F. (2010), “Implicit moment invariant,” *Int. J. Comput. Vis.*, 86, 72-86.
- [9] Refrégier, P., Javidi, B. (1995) “Optical image encryption based on input plane and Fourier plane random encoding”, *Opt. Lett.*, 20, 767-9.
- [10] Towghi, N., Javidi, B., Zuo, Z. (1999) “Fully-phase encryption image processor”, *J. Opt. Soc. Am. A* 16, 1915-27.
- [11] Millán, M. S., Pérez-Cabré, E., Javidi, B. (2006) “Multifactor authentication reinforces optical security,” *Opt. Lett.* 31, 721-3.
- [12] Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I. (2005) “Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys,” *Opt. Lett.*, 30, 1644-6.
- [13] Pratt, W. K. (1991) *Digital image processing*, 2nd ed. John Wiley & Sons, Inc., NY, USA.
- [14] Gonzalez, R. C., Woods, R. E., Eddins, S. L. (2004) *Digital image processing using matlab*, Pearson, Prentice Hall, NJ, USA.
- [15] Goodman, J. W. (1996) *Introduction to Fourier optics*, 2nd Edition, McGraw-Hill, NY, USA.
- [16] Mahajan, V. N. (1991) “Aberration theory made simple,” *SPIE Opt. Eng. Press*, Bellingham, WA, USA.

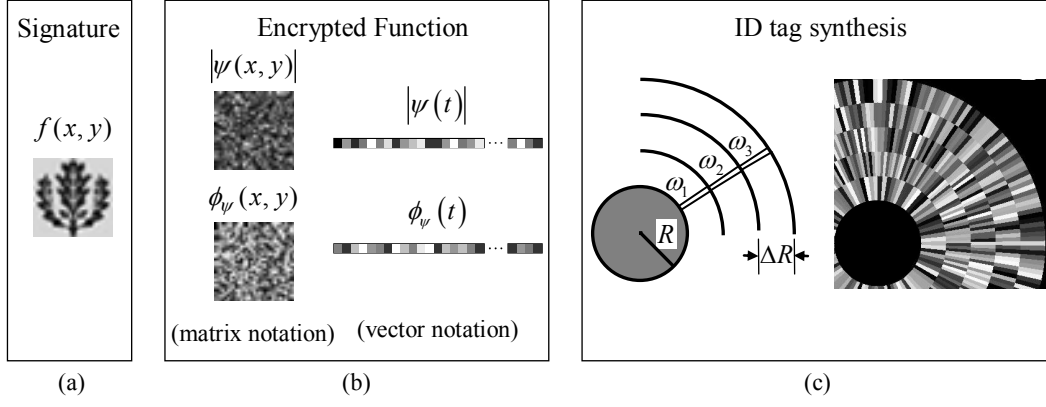


Figure 1. Generation of an optical ID tag: (a) primary image used as a signature; (b) amplitude and phase distributions of the encrypted signature using the FPE technique; (c) parameters used to define the concentric rings in the synthesis of the ID tag.

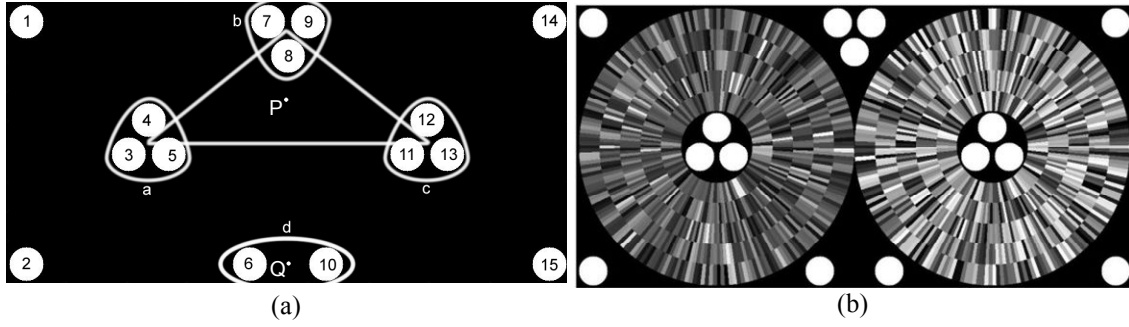


Figure 2. (a) Set of reference white dots used to determine the deformation of the captured ID tag. (b) Generated final ID tag from the encrypted signature shown in Fig. 1a and 1b.

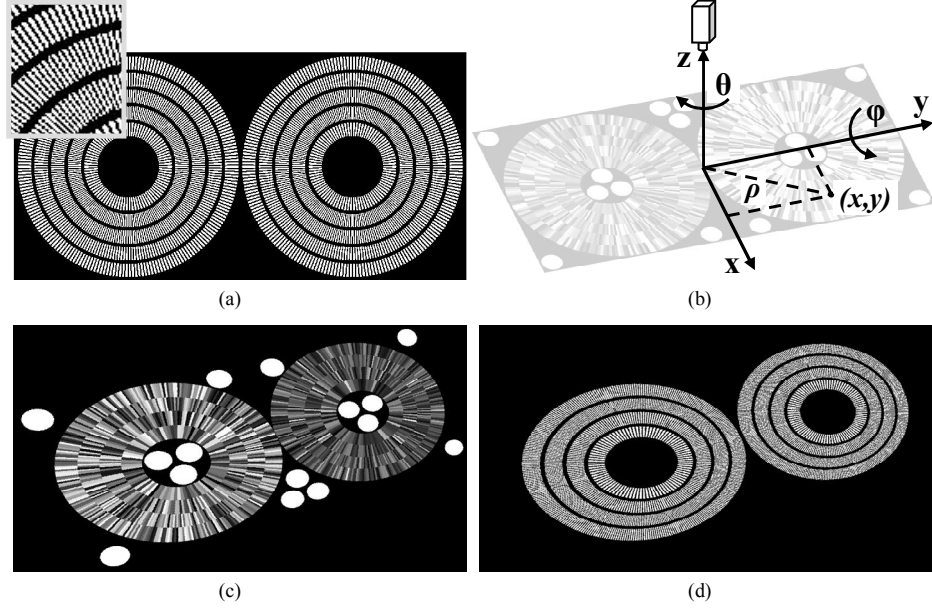


Figure 3. (a) Reading mask. A detailed area is shown on the upper left corner. (b) Angles θ and φ used to model deformations caused by perspective. Distance ρ is considered for distortions of the optical imaging system. (c) Captured ID tag under deformation of perspective with $\theta = 20^\circ$ and $\varphi = -30^\circ$. (d) Reading mask transformed using Eq. (2) with matrix \mathbf{T} determined from the reference white dots of Fig. 3c.

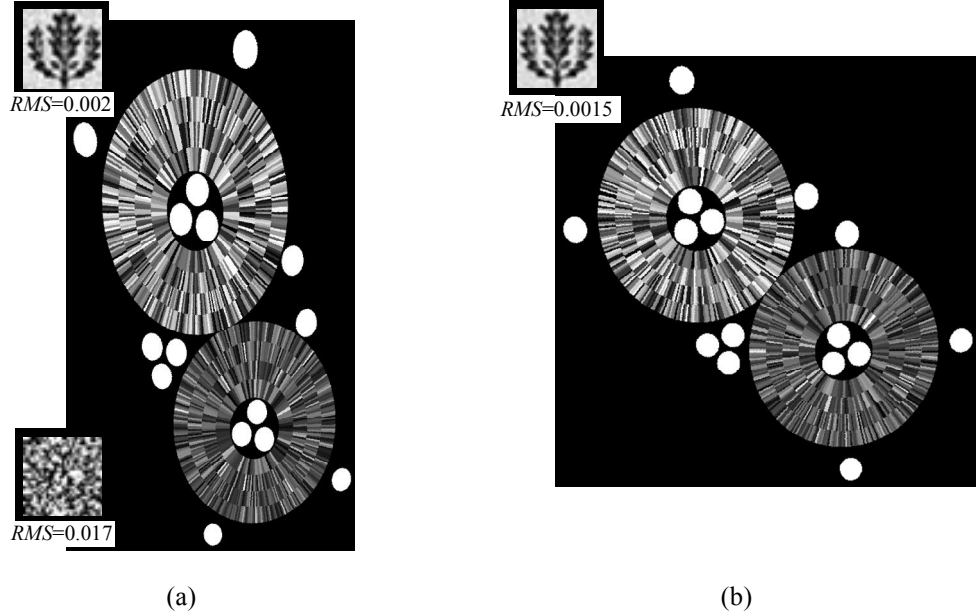


Figure 4. Captured ID tags when they are mainly deformed by perspective. On the upper left corner the retrieved signature is shown. (a) $\theta = 70^\circ$ and $\varphi = -30^\circ$; (b) $\theta = 40^\circ$ and $\varphi = -15^\circ$. On the bottom left corner of (a) the retrieved signal is displayed, corresponding to the case where the captured ID tag is converted back to its original orientation by using interpolation.

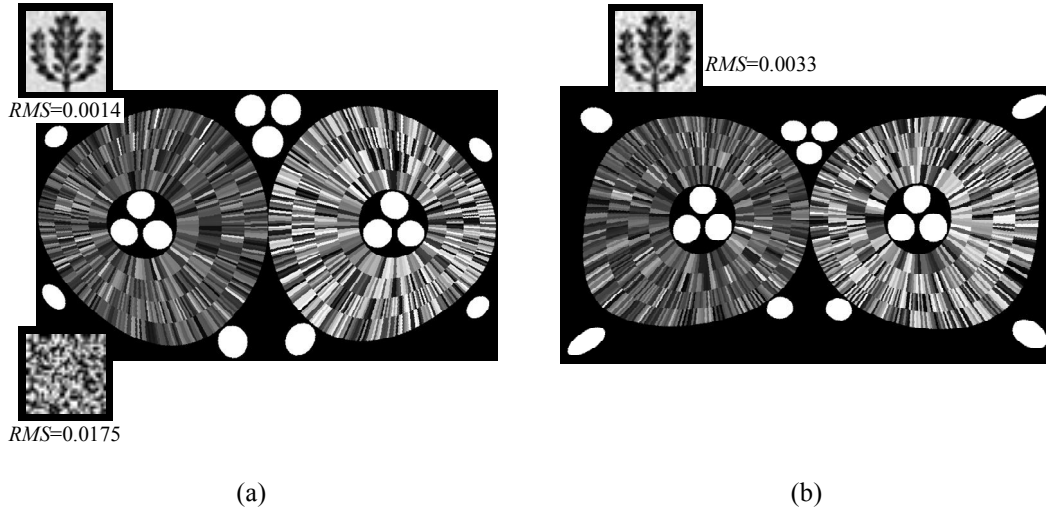


Figure 5. ID tags modified by distortion of the optical imaging system of the receiver: (a) barrel distortion ($a = 6 \cdot 10^{-7}$ in Eq. 4) and (b) pincushion ($a = -5 \cdot 10^{-7}$ in Eq. 4). On the upper left corner of the ID tag the retrieved signature is displayed. For (a), the obtained signal is displayed on the bottom left corner when the captured ID tag is compensated for distortion by using interpolation.

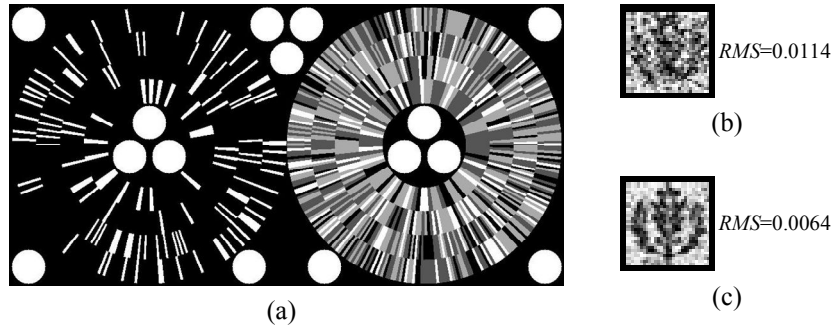
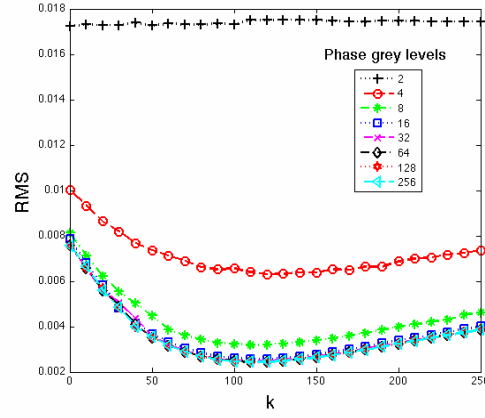
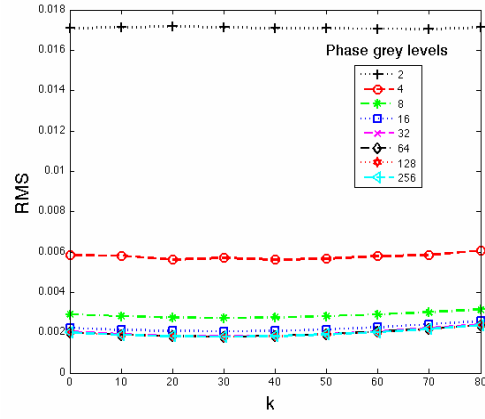


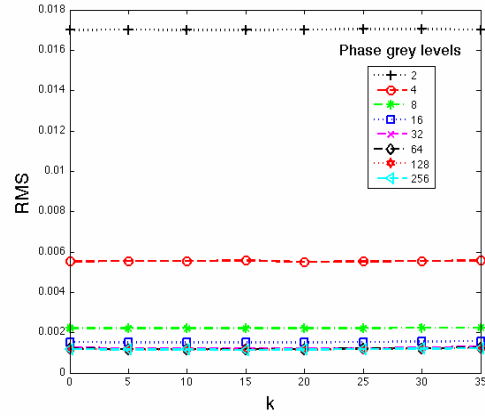
Figure 6. (a) ID tag with binary amplitude information (left optical disk) and phase distribution reproduced with 8 grey levels (right optical disk). Decrypted functions when the amplitude binary values are set to: (b) {0,1}, and (c) {1,2}. FPE is used in both examples.



(a)

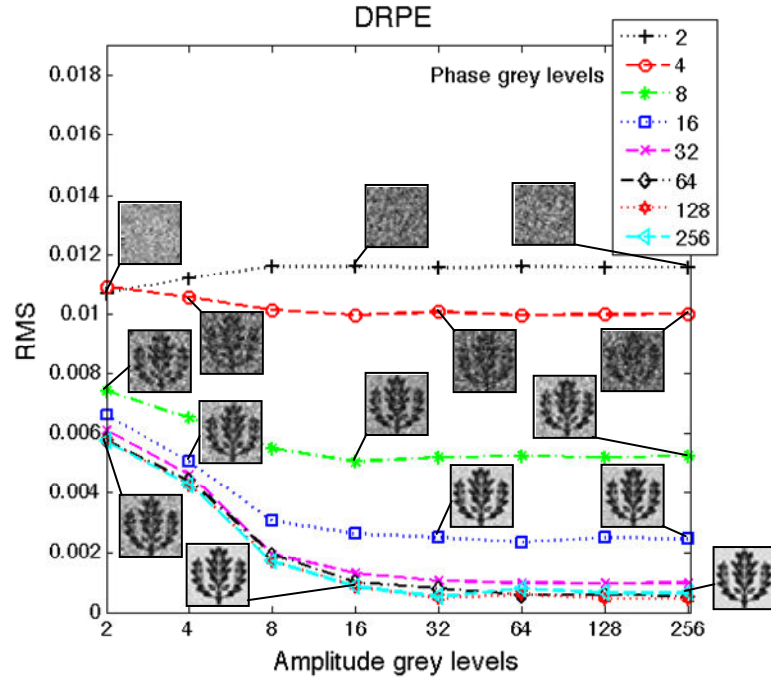


(b)

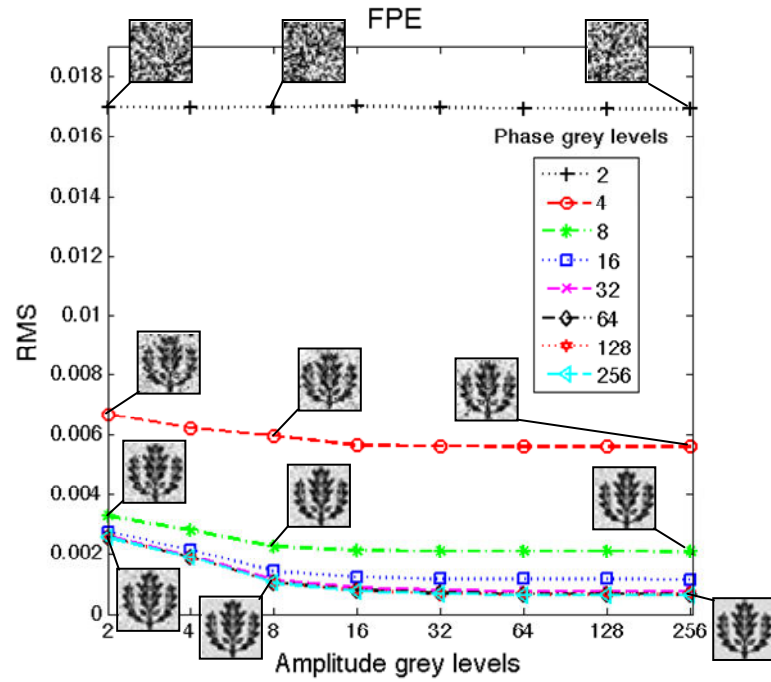


(c)

Figure 7. RMS values obtained for different values of the minimum grey level (k) used to discretize the amplitude information: (a) Binary amplitude with values $\{k, 255\}$ and different number of grey levels to display the phase distribution; (b) Amplitude information discretized with 4 grey levels $\{k, \frac{1}{3}255, \frac{2}{3}255, 255\}$; (c) Amplitude information discretized with 8 grey levels $\{k, \frac{1}{7}255, \frac{2}{7}255, \dots, 255\}$. In all the cases, the FPE method is used for encryption.



(a)



(b)

Figure 8. RMS results obtained when varying the number of grey levels used to codify the magnitude and the phase distribution of the encrypted information. (a) DRPE is used for encryption/decryption; (b) FPE is applied.

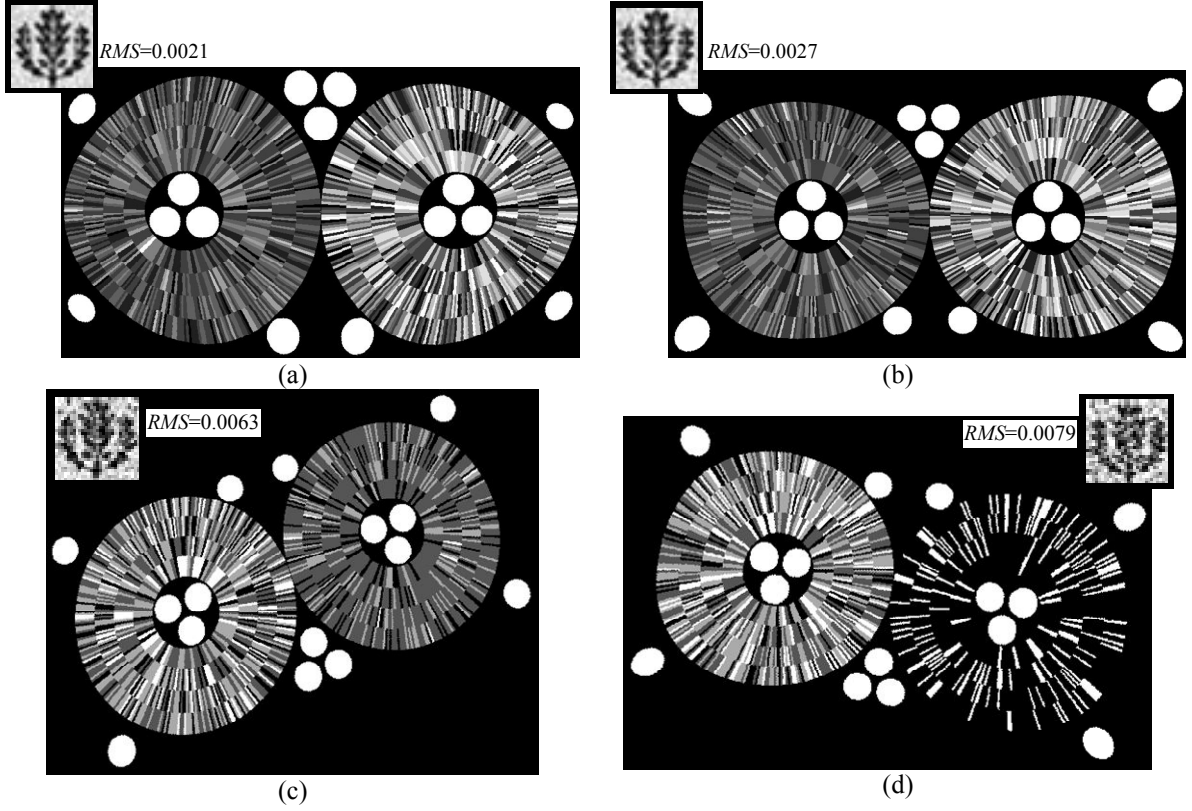


Figure 9. Degraded ID tag whose amplitude and phase information is reproduced with a limited number of grey levels. For all cases, the retrieved signature with the FPE technique is also shown: (a) Barrel distortion ($a = -4 \cdot 10^{-6}$), amplitude and phase both discretized with 8 grey levels. (b) Pincushion distortion ($a = 3 \cdot 10^{-6}$), amplitude and phase both discretized with 8 grey levels. (c) Perspective deformation ($\theta = -20^\circ$, $\varphi = 15^\circ$), amplitude and phase both discretized with 4 grey levels. (d) Pincushion distortion ($a = 2 \cdot 10^{-6}$) and perspective deformation ($\theta = 10^\circ$, $\varphi = 10^\circ$), binary amplitude and phase reproduced with 4 grey levels.